CLAIMS

1. A digital data storage subsystem for storing data in digital form comprising:

A. a storage medium configured to store digital data;

B. a storage control module configured to

i. in response to a storage request requesting storage of digital data, receive the digital data that is to be stored in response to the storage request from a source, encrypt the received digital data using a selected encryption key and enable the encrypted digital data to be stored on the storage medium; and

ii. in response to a retrieval request requesting retrieval of digital data, enable at least one selected portion of the encrypted digital data to be retrieved from the storage medium, decrypt the retrieved encrypted digital data using a selected decryption key, and provide the decrypted digital data to a destination; and

C. a sanitization control module configured to, in response to a sanitization request, make the decryption key unavailable to the storage control module, thereby disabling the storage control module from thereafter decrypting the encrypted digital data stored on the storage medium.

2. A digital data storage system as defined in claim 1 in which the storage medium is a magnetic medium, in which the encrypted digital data is stored in magnetic form.

3. A digital data storage system as defined in claim 2 in which the magnetic medium is a disk.

4. A digital data storage system as defined in claim 1 in which the storage medium is an electronic medium, in which the encrypted digital data is stored in electronic form.

5. A digital data storage system as defined in claim 1 in which the storage control module is configured to make use of a symmetric key encryption and decryption methodology in encrypting the digital data and decrypting the encrypted digital data.

6. A digital data storage system as defined in claim 1 in which the storage control module is configured to make use of an asymmetric key encryption and decryption methodology in encrypting the digital data and decrypting the encrypted digital data.

7. A digital data storage system as defined in claim 1, the digital data storage system further comprising a decryption key store configured to store the decryption key, and the storage control module is configured to make use of the decryption key stored in the decryption key store in decrypting the encrypted digital data.

8. A digital data storage system as defined in claim 7 in which the sanitation control module is configured to make the decryption key unavailable to the storage control module by wiping the decryption key from the decryption key store.

9. A digital data storage system as defined in claim 8 in which the sanitation control module is configured to wipe the decryption key from the decryption key store by erasing the decryption key store.

10. A digital data storage system as defined in claim 1, the digital data storage system further comprising a key generator configured to generate the decryption key.

11. A digital data storage system as defined in claim 10 in which the key generator module is configured to generate the decryption key from two bit patterns provided thereto using a predetermined generation methodology.

12 A digital data storage system as defined in claim 11 in which the key generator module is configured to generate the decryption key by concatenating the bit patterns together.

13. A digital data storage system as defined in claim 11 in which the key generator module is configured to generate the decryption key by exclusive-ORing the bit patterns together.

14. A digital data storage system as defined in claim 11 in which the key generator module is configured to store the decryption key in a decryption key store, and the sanitation control module is configured to make the decryption key unavailable by making the decryption key and at least one of the bit patterns unavailable.

15. A computer program product for use in connection with a processor to provide a sanitizing subsystem for sanitizing a digital data storage subsystem for storing data in digital form, the computer program product comprising:

A. a storage control module configured to enable the processor to

i. in response to a storage request requesting storage of digital data, receive the digital data that is to be stored in response to the storage request from a source, encrypt the received digital data using a selected encryption key and enable the encrypted digital data to be stored on the storage medium; and

ii. in response to a retrieval request requesting retrieval of digital data, enable at least one selected portion of the encrypted digital data to be retrieved from the storage medium, decrypt the retrieved encrypted digital data using a selected decryption key, and provide the decrypted digital data to a destination; and

B. a sanitization control module configured to enable the processor to, in response to a sanitization request, make the decryption key unavailable to the storage control module, thereby disabling the storage control module from thereafter decrypting the encrypted digital data stored on the storage medium.

16. A computer program product as defined in claim 15 in which the storage control module is configured to enable the processor to make use of a symmetric key encryption and decryption methodology in encrypting the digital data and decrypting the encrypted digital data.

17. A computer program product as defined in claim 15 in which the storage control module is configured to enable the processor to make of an asymmetric key encryption and decryption methodology in encrypting the digital data and decrypting the encrypted digital data.

18. A computer program product as defined in claim 15, in which the storage control module is configured to enable the processor to make use of the decryption key stored in a decryption key store in decrypting the encrypted digital data.

19. A computer program product as defined in claim 18 in which the sanitation control module is configured to enable the processor to make the decryption key unavailable to the storage control module by wiping the decryption key from the decryption key store.

20. A computer program product as defined in claim 19 in which the sanitation control module is configured to enable the processor to wipe the decryption key from the decryption key store by erasing the decryption key store.

21. A computer program product as defined in claim 15, the computer program product further comprising a key generator configured to enable the processor to generate the decryption key.

22. A computer program product as defined in claim 21 in which the key generator module is configured to enable the processor to generate the decryption key from two bit patterns provided thereto using a predetermined generation methodology.

23 A computer program product as defined in claim 22 in which the key generator module is configured to enable the processor to generate the decryption key by concatenating the bit patterns together.

24. A computer program product as defined in claim 22 in which the key generator module is configured to enable the processor to generate the decryption key by exclusive-ORing the bit patterns together.

25. A computer program product as defined in claim 22 in which the key generator module is configured to enable the processor to store the decryption key in a decryption key store, and the sanitation control module is configured to enable the processor to make the decryption key unavailable by making the decryption key and at least one of the bit patterns unavailable.

26. A method of operating a digital data storage subsystem for storing data in digital form, the method comprising:

A. a storage control step in which

i. in response to a storage request requesting storage of digital data, the digital data that is to be stored in response to the storage request from a source is received, encrypted using a selected encryption key and the encrypted digital data stored on a storage medium; and

ii. in response to a retrieval request requesting retrieval of digital data, retrieving least one selected portion of the encrypted digital data to be retrieved from the storage medium, decrypted using a selected decryption key, and the decrypted digital data being provided to a destination; and

B. a sanitization control step in which, in response to a sanitization request, the decryption key is made unavailable for decryption, thereby disabling the decryption of the encrypted digital data stored on the storage medium.

27. A method as defined in claim 26 in which the storage control step includes the step of making use of a symmetric key encryption and decryption methodology in encrypting the digital data and decrypting the encrypted digital data.

18. A method as defined in claim 26 in which the storage control step includes the step of making of an asymmetric key encryption and decryption methodology in encrypting the digital data and decrypting the encrypted digital data.

29. A method as defined in claim 26, in which the storage control step includes the step of making use of the decryption key stored in a decryption key store in decrypting the encrypted digital data.

30. A method as defined in claim 29 in which the sanitation control step includes the step of making the decryption key unavailable by wiping the decryption key from the decryption key store.

31. A method as defined in claim 30 in which the sanitation control step includes the step of wiping the decryption key from the decryption key store by erasing the decryption key store.

32. A method as defined in claim 26, the method further comprising a key generator step of generating the decryption key.

33. A method as defined in claim 32 in which the key generator step includes the step of generating the decryption key from two bit patterns provided thereto using a predetermined generation methodology.

34. A method as defined in claim 33 in which the key generator step includes the step of generating the decryption key by concatenating the bit patterns together.

35. A method as defined in claim 33 in which the key generator step includes the step of generating the decryption key by exclusive-ORing the bit patterns together.

36. A method as defined in claim 33 in which the key generator step includes the step of storing the decryption key in a decryption key store, and the sanitation control step includes the step of making the decryption key unavailable by making the decryption key and at least one of the bit patterns unavailable.